UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,005	10/30/2003	Michael Scheidell	1012-003U	1429

29973 7590 11/12/2008
CAREY, RODRIGUEZ, GREENBERG & PAUL LLP
ATTN: STEVEN M. GREENBERG, ESQ.
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2431	
MAIL DATE	**DELIVERY MODE**
11/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/699,005	**Applicant(s)** SCHEIDELL, MICHAEL	
	Examiner AREZOO SHERKAT	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 August 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-11 and 14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-11 and 14* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Reopening of Prosecution - New Ground of Rejection After Appeal Brief

In view of the Appeal Brief filed on 3/31/2006, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 9-11 and 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Lyle et al., (U.S. Patent No. 6,971,028 and Lyle hereinafter).

Regarding claim 9, Lyle discloses a computer network intrusion detection system comprising:

a plurality of different log analyzers for different external networks (i.e., tracking system computers)(col. 6, lines 17-30), each log analyzer being configured for detecting attacks upon a firewall (i.e., wherein a firewall is a network element) in a corresponding one of the different external networks defining an edge detection network (Figure 1- col. 4, lines 49-67 and col. 5, lines 1-67);

an edge database log coupled to the different log analyzers logging attacks upon the different external networks (i.e., a trusted third party intermediary configured to receive the handoff message and pass it on to the other administrative domain ... The event manager 306 also supplies event data to the log database 320 as it is received either from the handoff receiver 302 or from the sniffer module 304)(col. 16, lines 4-40 and col. 7, lines 43-57), an intrusion detector (i.e., the sniffer module)coupled to a client network and configured to detect external attacks upon the client network, an analyzer (i.e., the analysis framework module) coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log (i.e., The analysis framework 308 also determines whether an event is associated with an existing event or group of related events, and associates related events into a single incident software object. Events that are not related to any other events are associated with a new incident object and may be later grouped with subsequently-received event data that is related to the same incident)(col. 7, lines 43-67 and col. 8, lines 1-14), and

a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks (i.e., alerting module)(col. 8, lines 15-33 and col. 14, lines 21-48),

a second intrusion detector for detecting external attacks upon a second computer network (i.e., the handoff receiver module), and a second analyzer (i.e., the analysis framework module) coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof (i.e., the analysis framework module tests for vulnerabilities by analyzing data from the sniffer module and the handoff receiver module, wherein the sniffer module monitors a port in the local administrative domain and the handoff receiver module monitors a port to which another administrative domain is directed to send handoff information regarding an attack)(col. 9, lines 60-67, and col. 10, lines 1-67 and col. 11, lines 1-11), wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison (i.e., The analysis framework 308 also determines whether an event is associated with an existing event or group of related events, and associates related events into a single incident software object. Events that are not related to any other events are associated with a new incident object and may be later grouped with subsequently-received event data that is related to the same incident)(col. 7, lines 43-67 and col. 8, lines 1-33). "generating a specific attack alert in response to a substantial absence of similarity in the comparison" is merely a policy that, as a design choice, may well be defined in the policy database 326. The policy database is therefore consulted to dictate how certain types of events and incidents should be processed by the analysis framework 308, including the responsive action, if any, to be taken by the analysis framework. Therefore, depending on the defined policy the alerting module is instructed to generate alerts based on different triggering events.

Regarding claim 10, Lyle discloses the system according to claim 9 further comprising an alert generator for generating an alert indicative of the specific attack on the one of the networks experiencing the attacks having the absence of similarity of attacks on the other of the networks (i.e., alerts are generated as a result of the analysis framework module processing data from the sniffer module, monitoring a port in the local administrative domain, and the handoff receiver module, monitoring a port to which another administrative domain is directed to send handoff information regarding an attack. Note that "attacks having the absence of similarity of attacks on the other of the networks" are new/single incidents that are not related to any existing incidents)(col. 13, lines 19-67 and col. 14, lines 1-48).

Regarding claim 11, Lyle discloses the system according to claim 9.

Lyle further discloses a vulnerability tester coupled to said filter for testing the one of the networks not experiencing the attacks for a vulnerability to the attack characteristic experienced by the other of the computer networks (i.e., wherein the sniffer module continuously assesses whether the data being scanned is suspicious, in the sense that it indicates that an attack may be taking place. The sniffer module may also search for other information, clues, or signatures previously associated with attacks on the network being protected or ***other networks.*** Therefore, the analysis framework module tests for vulnerabilities by analyzing data from the sniffer module and the handoff receiver module, wherein the sniffer module monitors a port in the local administrative domain and the handoff receiver module monitors a port to which another administrative domain is directed to send handoff information regarding an attack)(col. 9, lines 60-67, and col. 10, lines 1-67 and col. 11, lines 1-11).

Regarding claim 14, Lyle discloses a method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

logging attacks on multiple different external networks defining an edge detection network (i.e., a trusted third party intermediary configured to receive the handoff message and pass it on to the other administrative domain ... The event manager 306 also supplies event data to the log database 320 as it is received either from the handoff receiver 302 or from the sniffer module 304)(col. 16, lines 4-40 and col. 7, lines 43-57),

detecting an attack on a client network (i.e., the analysis framework module tests for vulnerabilities by analyzing data from the sniffer module and the handoff receiver module, wherein the sniffer module monitors a port in the local administrative domain and the handoff receiver module monitors a port to which another administrative domain is directed to send handoff information regarding an attack)(col. 9, lines 60-67, and col. 10, lines 1-67 and col. 11, lines 1-11), classifying the attack as either a general attack or a client specific attack by comparing the attack to attacks logged for the edge detection network (i.e., The analysis framework 308 also determines whether an event is associated with an existing event or group of related events, and associates related events into a single incident software object. Events that are not related to any other events are associated with a new incident object and may be later grouped with subsequently-received event data that is related to the same incident)(col. 7, lines 43-67 and col. 8, lines 1-14), prioritizing handling of the detected attack if the attack is classified as a general attack (i.e., depending on the policies defined in the policy database 326, an attack may be logged but otherwise ignored while another attack is dealt with immediately), and generating a second alert in response to the presence of the match wherein the first alert is indicative of a specific attack on the first network and the second alert is indicative of a non-specific attack on the first network (i.e., "generating a specific attack alert in response to a substantial absence of similarity in the comparison" is merely a policy that, as a design choice, may well be defined in the policy database 326. The policy database is therefore consulted to dictate how certain types of events and incidents should be processed by the analysis framework 308, including the responsive action, if any, to be taken by the analysis framework. Therefore, depending on the defined policy, the alerting module is instructed to generate alerts based on different triggering events)(col. 7, lines 43-67 and col. 8, lines 1-33).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Please see the attached PTO-892 for details.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AREZOO SHERKAT whose telephone number is (571)272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Arezoo Sherkat/
Patent Examiner
Group 2431
Nov. 4, 2008
/Syed Zia/
Primary Examiner, Art Unit 2431
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435